UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,396	02/18/2004	Sourabh Satish	SYMAP043	4350

69417 7590 10/13/2009

HUNTON & WILLIAMS LLP / SYMANTEC CORPORATION
INTELLECTUAL PROPERTY DEPT.
1900 K STREET, NW
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,396	SATISH, SOURABH	
	Examiner	Art Unit	
	PAUL CALLAHAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18 and 29-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18, 29-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is directed towards the Applicant's response filed 5-19-2009. Claims 1-18 and 29-38 are pending in the instant application and have been examined.

Response to Arguments

2. Applicant's arguments filed 5-19-2009 have been fully considered but they are not persuasive.

The Applicant argues that the claimed invention may be distinguished from the teachings of Schultz 2003/0065926 A1, and Jordan 7,210,040, by asserting that the combination fails to teach the feature of observing that a process started by an executable has either performed or has attempted to perform an action with which a second risk level, being higher than the first, is associated.

The Examiner disagrees with this assessment of the applied references. For example, as the Applicant points out in the arguments presented with the latest amendment, Jordan teaches the steps of allowing an executable to execute in an emulation environment, and evaluates any process started by the executable for risk (figure 2, col. 5 lines 35-40). The Applicant's claim is not specific in excluding an emulator as the execution environment for the executable, and the Examiner maintains that the cited section of Jordan therefore does read on this feature of the claimed invention. The Examiner notes that the claim language includes the phrase "attempts to perform" and therefore an emulation environment would read on the claim language as

an executable permitted to execute in this environment will "attempt" to initiate a process.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-6, 18, 37, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schultz et al., US 2003/0065926 A1, and Jordan, 7,210,040.

As for claim 1, Schultz teaches a method for providing computer security, comprising: determining, using a processor, whether an executable associated with a static state meets a predetermined criterion [0021], [0022]; associating a first risk level with the executable [0038], if it is determined that the executable meets the predetermined criterion [0040]; observing that a process started by the executable has performed or has attempted to perform an action with which a second risk level, being higher than the first, is associated [0108], updating the first risk level to the second risk level, based on the observation, and performing a predetermined responsive action with respect to the process if the second risk level exceeds the threat detection threshold [0022], [0023]; wherein determining whether the executable meets the

predetermined criterion does not compare the executable with a virus signature [0042]. Schultz does not explicitly disclose the step wherein the step of updating the first risk level to a second risk level higher than the first if a process started by the executable has been allowed to execute. However, Jordan does teach this step wherein a process started by an executable is permitted to execute prior to a determination being made as to the risk associated with that process (figure 2, col. 5 lines 35-40). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Schultz. It would have been obvious to do so since this would allow for monitoring in real time any suspicious executable files and increase the accuracy of risk detection.

As for claims 37 and 38: Claim 37 represents the apparatus configured to carry out the method steps of claim 1, Claim 38 represents the computer-program product that instructs a processor to undertake the method steps of claim 1. Claims 37 and 38 recite substantially the same limitations as claim 1 and are thereby rejected on the same basis as that claim.

As for claim 2, Schultz discloses the method for providing computer security, wherein the risk level indicates a level of potential risk that will be brought by operating the executable (para. 0038, lines 3-6).

As for claim 3, Schultz discloses the method for providing computer security, wherein the risk level indicates how much risk the executable presents (para. 0099, lines 1-15; para. 0100, lines 1-3).

As for claim 4, Schultz discloses the method for providing computer security, wherein the predetermined criterion includes a configuration criterion (para. 0036, lines 11-14; para. 0119, lines 8-18).

As for claim 5, Schultz discloses the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable is configured as a service (para. 0103, lines 3-4).

As for claim 6, Schultz discloses the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable is configured to run under a high privileged account (para. 0040, lines 4-8).

As for claim 18, Schultz discloses the method for providing computer security comprising associating with the executable a risk type indicating a type of risk to which the executable is vulnerable (para. 0038, lines 4-8; para. 0099, lines 4-12).

5. Claims 7, 8, 10, 12-17 and 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schultz and Jordan, and further in view of Tajalli et al. (US 2004/0143749 A1).

As for claim 7, Schultz and Jordan disclose all the limitations of claim 7 except where the predetermined criterion is used to determine whether the executable is installed via a standard procedure. The general concept of whether the executable is installed via standard procedure is well known in the art as illustrated by Tajalli, which discloses controlling access to system resources by each process bases on a behavior control description for the process set to which it belongs (para. 0020, lines 5-7). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to in clued the use of a predetermined criterion to determine if the executable has not properly installed in order to prevent malicious code execution on a computer system, as well as to controlling access over malicious code.

As for claim 8, Schultz and Jordan disclose all the limitations of claim 8 except the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has sufficient access control. The general concept of determining if the executable having sufficient access control is well known in the art as illustrated by Tajalli, which discloses access control engine to monitor access and

use of critical system resources, in addition the IDS watches applications request and resources used, looking for request or uses that depart from acceptable use and behavior (para. 0081, lines 1-11; para. 0161, lines 12-14; para. 0175, lines 5-6). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining sufficient access control in order to control access rights to system resources.

As for claim 10, Schultz and Jordan disclose all the limitations of claim 10, except the method of providing computer security, wherein the predetermined criterion is used to determine whether the executable is signed. The general concept of determining if the executable is signed is well known in the art as illustrated by Tajalli, which disclose that the IDS will check for encryption within the executable (para. 0161, lines 12-14; para. 0169, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if the executable is signed in order to determine the origin of the executable, as public key cryptography bind the signer to the key.

As for claim 12, Schultz and Jordan disclose all the limitations of claim 12 except providing compute security wherein, the predetermined criterion includes a capability criterion. The general concept of the predetermined criterion includes a capability criterion is well known in the art as illustrated by Tajalli, which discloses the

predetermined criterion include capability (para. 0055, lines 1-2; para. 0175, lines 5-6). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of a capability criterion in order to protect the system against attack.

As for claim 13, Schultz and Jordan disclose all the limitations of the claim except the method for providing computer security wherein the predetermined criterion is used to determine whether the executable has networking capability. The general concept of determining if the executable has network capability is well known in the art as disclosed by Tajalli, which discloses network protection against malicious codes (para. 0244, lines 1; 0251, lines 2-9; para. 0175, lines 5-6). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if malicious code has network capability in order to protect the network against malicious codes that may cause damage to a network.

As for claim 14, Schultz and Jordan disclose all the limitations of claim 14 except the method for providing computer security, wherein the predetermined criterion is used to monitor whether the executable has privilege manipulation capability. The general concept of determining whether the executable has privilege manipulation capability is well known in the art as illustrated by Tajalli, which discloses that the IDS would define modifying or manipulating registry keys as inappropriate behavior that would be blocked

(para. 0050, lines 1-8). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if executable has privilege manipulation Capability in order to protect the system against malicious codes that may want to modify system registries.

As for claim 15, Schultz and Jordan disclose all the limitations of claim 15 except the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has remote process capability. The general concept of determining if the executable has remote process capability is well known in the art as illustrated by Tajalli, which discloses the IDS is configured to control network services to include remote connection (para. 0236, lines 1-3; para. 0239, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if malicious code has remote capability in order to prevent the network from being taking over by hackers that may use Trojan Horses to enter the network unchecked.

As for claim 16, Schultz and Jordan disclose all the limitations of claim 16 except the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has process launching capability. The general concept of determining if the malicious code has process launching capability is well known in the art as illustrated by Tajalli, which discloses a malicious code initiate HTTP

connection to other Web servers (para. 0244, lines 1-2; para. 0249, lines 1-2). Therefore it would have been obvious for one ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if the malicious code has process launching capability in order to stop malicious code from executing and from calling other system resources from the network.

As for claim 17, Schultz and Jordan disclose all the limitation of the claim except the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has secure algorithm. The general concept of determining if malicious codes has secure algorithm is well known in the at as illustrated by Tajalli, which discloses the IDS controls access to any attributes of files or directories including if encryption present for the malicious code (para. 0217, lines 1-2; para. 0222, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if the malicious code has secure algorithm, in order to protect against virus that uses encrypted code to hide their payload from virus protection mechanism.

As for claim 29-31, Schultz and Jordan disclose all the limitation of the claims except the method for providing computer security comprising analyzing historical evidence; the historical evidence include a record of activities and log file. The general concept of analyzing historical evidence is well known in the art as illustrated by Tajalli,

which discloses the use of historical evidence (para. 0091, lines 1-7; para 0097, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of analyzing historical evidence, record activities and log file in order to assign processes into their proper category, thus that new policy may be implemented more effectively.

As for claim 32, Schultz and Jordan disclose all the limitations of the claim except the method for providing computer security wherein the historical evidence includes a system optimization file. The general concept of the historical includes a system optimization file is well known in the art by Tajalli, which disclose a communication module to retrieve configuration or log data and returns them, in addition the communication module can retrieve data from disk or from the engine, and request alert when unusual event occur (para 0090, lines 3-8). System optimization file or swap files resides on disk. Therefore it would have been obvious for one of ordinary skill in that art at the time of the invention to modify Schultz to include the use of swap file in order to obtain information that are relevant to build system policy.

As for claims 33 and 34, Schultz and Jordan disclose all the limitation of the claims except the method for providing computer security, wherein historical evidence includes a crash dump. The general concept of the historical evidence includes a crash dump is well known in the art as illustrated by Tajalli, which discloses a communication

module that monitors local log files, transfers log data to a management infrastructure and request alerts when unusual events occur (para. 0090, lines 3-8). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use a crash dump file and prefetch file in order to gather information when system failure occur.

6. Claims 9, 11, 35, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schultz and Jordan in view of Khazan et al. (US 2005/0108562 A1).

As for claims 9 and 11, Schultz and Jordan disclose all the limitations of the claims except the method of providing computer security wherein the predetermined criterion is used to determine whether the executable is recent and determine whether the executable has a modified date different from the created date. The general concept of determining whether the executable is recent and determining whether the executable has a modified date different from the created date is well known in the art .as illustrated by Khazan, which discloses analyzing the executable when modification take place (para. 0107, lines 14; para. 0115, lines 1-19). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of Khazan in order to verify whether modification has taken place within the executable.

As for claims 35 and 36, Schultz and Jordan discloses all the limitation of the claims except the method for providing computer security, comprising performing a dynamic risk analysis, and determining whether an action is required. The general concept of performing dynamic analysis and determining whether an action is required is well known in the art as illustrated by Khazan, which discloses static and dynamic analyzer (para. 0040, lines 12-13, and whether an action is required (para. 0099, lines 7-11, lines 21-26). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of dynamic analyzer to determine whether an action is required in order to protect compute systems against malicious codes.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/PEC/
AU2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437